Xpio HEALTH

Strengthening Cybersecurity in Healthcare: Essential and Enhanced Goals

Strengthening Cybersecurity in Healthcare:
Essential and Enhanced Goals

Healthcare organizations face ongoing cybersecurity challenges, and as technology becomes integral to managing patient data, ensuring strong cybersecurity measures is crucial. At Xpio Health, we specialize in providing technology solutions that enhance healthcare services, particularly in optimizing Electronic Health Records (EHR) systems, data visualization, performance management, and ensuring cybersecurity and compliance.

Here are Xpio Health's recommended essential and enhanced cybersecurity goals, aligned with the 2024 Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals set forth by the Department of Health and Human Services (HHS). These goals help healthcare organizations safeguard their systems and protect patient data effectively.

ESSENTIAL
Goals for Cybersecurity

Essential cybersecurity goals focus on building a robust defense against common threats. By addressing known vulnerabilities, securing email communications, implementing multifactor authentication, providing basic cybersecurity training, and ensuring strong data encryption, organizations can significantly reduce the risk of cyberattacks. These goals establish a strong baseline of security practices, creating a resilient infrastructure to protect sensitive patient data and maintain operational integrity.

Mitigate Known Vulnerabilities

The first step toward robust cybersecurity is addressing known vulnerabilities within your IT infrastructure. Think of your IT infrastructure as the foundation of your healthcare organization—if there are cracks in this foundation, it becomes vulnerable to external threats. Regularly assessing and managing these vulnerabilities is like performing routine maintenance on a building to ensure it remains secure and resilient.

Actionable Steps:

Conduct quarterly vulnerability scans.

Implement an endpoint protection platform.

Develop a vulnerability management plan to address identified issues promptly.

This process involves:

- Host/Server-Based Scanning: Implement tools to scan and identify vulnerabilities in servers and endpoints.
- Proactive Measures Against Insider Threats: Educate employees on the dangers of social engineering and implement strict access controls.

Threats Mitigated:

- Ransomware
- Social Engineering
- Insider Threat
- Attacks on network connected devices

Email Security

Email continues to be a major gateway for cyberattacks as hackers often use it to launch phishing scams, spoof emails, and spread other malicious activities. Imagine receiving an email that looks like it's from a trusted source such as a colleague or a bank, but it's actually a cleverly disguised attempt to steal your sensitive information. This is why enhancing email security is critical.

Actionable Steps:

Actionable Steps:

Implement an email filtering solution.

Mandate MFA for all email accounts.

Schedule bi-annual cybersecurity awareness training for all staff.

This process involves:

- Email Protection Systems: Deploy tools to filter and block malicious emails.
- Multifactor Authentication (MFA): Require MFA for email access to add an extra layer of security.
- Workforce Education: Conduct regular training sessions to educate employees about recognizing and avoiding email-based threats.

Threats Mitigated:

- Ransomware or other malware delivered via email
- Spoofing email attempts
- Account takeover

Multifactor Authentication (MFA)

Multifactor Authentication (MFA) is a crucial security measure that enhances protection for sensitive systems and data by requiring multiple forms of verification. Think of it like securing a valuable item with both a lock and an alarm system—if one fails, the other still protects you. Implementing MFA reduces the risk of unauthorized access by adding an extra hurdle for potential attackers.

Actionable Steps:

Deploy MFA across all critical applications.

Regularly audit and manage credentials.

Educate users on the importance and use of MFA.

This process involves:

- Implementation of MFA: Require MFA for accessing critical systems, especially those accessible from the internet.
- Identity and Credential Management: Ensure all identities and credentials are issued, managed, and audited regularly.

Threats Mitigated:

- Lateral movement within an environment
- Account takeover

Basic Cybersecurity Training

Human error contributes to many cybersecurity breaches, often due to a lack of awareness about potential threats. Without proper training, employees might inadvertently click on phishing links, use weak passwords, or mishandle sensitive information. Providing basic cybersecurity training equips organizational users with the knowledge and skills needed to recognize and avoid these risks, fostering a more secure work environment.

Actionable Steps:

Create a comprehensive cybersecurity training program.

Provide quarterly training sessions for all employees.

Offer specialized training for IT staff and other privileged users.

This process involves:

- Training Programs: Develop training modules tailored to different roles within the organization.
- Role-Specific Training: Privileged users should receive additional training on their specific security responsibilities.

Threats Mitigated:

- Ransomware
- Social engineering
- Insider threat
- Attacks on network connected devices

Strong Encryption

Encrypting data both in transit and at rest is crucial to protecting sensitive information from unauthorized access. Imagine sending a confidential letter through the mail—without encryption, it's like sending it without an envelope, exposing its contents to anyone who intercepts it. Encryption acts as a secure envelope, ensuring that even if the data is intercepted, it remains unreadable and safe.

Actionable Steps:

Use TLS/SSL for data in transit.

Encrypt sensitive data stored on servers and backups.

Regularly review and update encryption protocols.

This process involves:

- Data Encryption: Implement strong encryption protocols for data in transit and at rest to maintain confidentiality and integrity.
- Regular Audits: Conduct regular audits to ensure encryption standards are met and updated as necessary.

Threats Mitigated:

- Data theft
- Inbound attack email filtering

Revoke Credentials Promptly

Revoking access credentials promptly for departing employees, contractors, and affiliates is vital to maintain security. When someone leaves the organization, their access to sensitive systems must be removed immediately to prevent unauthorized use. Failure to do so can leave the organization vulnerable to breaches and data theft by former insiders. Ensuring these credentials are swiftly revoked is a key part of a robust cybersecurity strategy.

Actionable Steps:

Automate the deprovisioning process.

Conduct monthly audits of access logs.

Train HR and IT staff on deprovisioning procedures.

This process involves:

- Deprovisioning Procedures: Establish and enforce procedures to promptly revoke access upon termination of employment or contracts.
- Regular Audits: Regularly audit access logs to ensure compliance with deprovisioning procedures.

Threats Mitigated:

- Lateral movement within an environment
- Account takeover

Basic Incident Planning and Preparedness

Being prepared for cybersecurity incidents is essential for healthcare organizations. Imagine if a hospital's systems were suddenly compromised, disrupting patient care and jeopardizing sensitive information. Without a solid incident response plan, recovery could be slow and chaotic, leading to severe consequences. By planning ahead, healthcare providers can quickly address threats, minimize damage, and restore normal operations efficiently.

Actionable Steps:

Develop a comprehensive incident response plan.

Conduct annual incident response drills.

Establish a communication plan for incident response.

This process involves:

- Incident Response Plan: Develop and regularly update an incident response plan.
- Stakeholder Coordination: Ensure all relevant stakeholders are aware of their roles in the event of an incident.

Threats Mitigated:

- Patient safety
- Business continuity
- Unplanned operational downtime

Unique Credentials

Using unique credentials within the organization's network is essential for security. When each user has a distinct set of login details, it becomes easier to spot unusual activities and unauthorized access. This approach prevents attackers from moving freely within the network if they gain access. By isolating credentials, organizations can quickly identify and respond to threats, minimizing potential damage.

Actionable Steps:

Issue unique credentials for all users.

Regularly review and update credential policies.

Implement network segmentation to enhance security.

This process involves:

- Credential Management: Issue unique credentials for each user and regularly audit them.
- Network Segmentation: Implement network segmentation to limit access to sensitive areas.

Threats Mitigated:

- Lateral movement within an environment

Separate User and Privileged Accounts

Separating user accounts from privileged accounts is crucial for minimizing the risk of unauthorized access to critical systems. Think of it as having different keys for different doors in a building: one for general areas and another for high-security rooms. By ensuring that only specific accounts have access to sensitive data and administrative functions, organizations can better protect against security breaches and internal threats.

Actionable Steps:

Create separate accounts for administrative and user tasks.

Use privileged access management tools.

Conduct regular reviews of account permissions.

This process involves:

- Secondary Accounts: Establish secondary accounts for administrative tasks.
- Access Controls: Implement strict access controls to manage privileged accounts.

Threats Mitigated:

- Lateral movement within an environment
- Account takeover

Vendor/Supplier Cybersecurity Requirements

Third-party vendors and suppliers often access sensitive systems and data, which can introduce significant cybersecurity risks. If a vendor's security is compromised, it can create vulnerabilities in your organization. To protect against these potential threats, it's crucial to implement strict cybersecurity requirements for all vendors and suppliers. By doing so, you can mitigate the risks they pose and ensure your data remains secure.

Actionable Steps:

Develop a vendor assessment program.

Include cybersecurity clauses in all vendor contracts.

Regularly review and update vendor security policies.

This process involves:

- Vendor Assessment: Regularly assess and monitor the cybersecurity practices of third-party vendors.
- Contractual Obligations: Include cybersecurity requirements in vendor contracts.

Threats Mitigated:

- Supply chain risk

ENHANCED

Goals for Cybersecurity

Once essential cybersecurity measures are in place, healthcare organizations should aim to enhance their security posture further. Enhanced goals focus on proactive strategies like maintaining a detailed asset inventory, enforcing third-party vulnerability disclosures, conducting regular cybersecurity testing, and implementing centralized log collection. By adopting these advanced practices, organizations can detect and mitigate sophisticated threats more effectively, ensuring a higher level of security and preparedness. These goals represent a commitment to continuous improvement in cybersecurity, protecting both patient data and organizational assets in an ever-evolving threat landscape.

Asset Inventory

Keeping track of all IT assets is crucial for effective management and security in healthcare organizations. Imagine trying to protect a house without knowing all its entry points—it's nearly impossible. Similarly, without a detailed inventory of hardware and software, identifying vulnerabilities and responding to threats becomes challenging. Ensuring every device and application is accounted for helps mitigate risks and enhances overall cybersecurity.

Actionable Steps:

Implement an IT asset management system.

Conduct quarterly asset inventory reviews.

Integrate asset inventory with security management tools.

This process involves:

- Inventory Management: Use automated tools to discover and inventory all hardware and software assets.
- Regular Updates: Ensure the asset inventory is regularly updated to reflect changes.

Threats Mitigated:

- Shadow assets not covered under critical processes like vulnerability management
- Shadow IT

Third-Party Vulnerability Disclosure and Incident Reporting

Establishing processes for vendors to report vulnerabilities and incidents promptly is crucial for maintaining a secure healthcare environment. When vendors can quickly report issues, healthcare organizations can address them before they escalate into major security breaches. This proactive approach ensures that potential threats are managed efficiently, protecting sensitive patient data and maintaining trust in the system.

Actionable Steps:

Develop a third-party vulnerability disclosure policy.

Establish clear incident reporting procedures for vendors.

Conduct regular reviews of vendor compliance.

This process involves:

- Vulnerability Disclosure: Require vendors to disclose known vulnerabilities.
- Incident Reporting: Ensure vendors have robust incident reporting mechanisms.

Threats Mitigated:

- Supply chain risk
- Asset compromise
- Unplanned outages
- Unplanned operational downtime

Cybersecurity Testing

Regular cybersecurity testing is essential for healthcare organizations to identify and address vulnerabilities before they can be exploited by malicious actors. Just like regular health check-ups help catch potential issues early, cybersecurity tests such as penetration testing and attack simulations reveal weak points in your systems. These proactive measures ensure that defenses are strong and ready to withstand potential attacks.

Actionable Steps:

Schedule bi-annual penetration tests.

Conduct annual attack simulations.

Share findings with relevant stakeholders and take corrective actions.

This process involves:

- Penetration Testing: Conduct regular penetration tests to identify security weaknesses.
- Attack Simulations: Perform attack simulations to test response capabilities.

Threats Mitigated:

- Unplanned operational downtime

Cybersecurity Mitigation

Effective cybersecurity mitigation is crucial for protecting sensitive data and maintaining system integrity. When vulnerabilities are discovered through penetration testing and attack simulations, they must be addressed promptly to prevent potential breaches. This proactive approach ensures that weaknesses are fixed before they can be exploited by cyber attackers. Quick and efficient mitigation efforts are essential to maintaining a secure healthcare environment and safeguarding patient information.

Actionable Steps:

Develop a plan for addressing high-priority vulnerabilities.

Assign responsibilities for remediation tasks.

Regularly review and update mitigation strategies.

This process involves:

- Vulnerability Remediation: Establish processes to prioritize and remediate identified vulnerabilities.
- Continuous Improvement: Implement feedback loops to improve security measures continuously.

Threats Mitigated:

- Unplanned operational downtime

Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures (TTP)

Detecting and responding to threats is crucial for healthcare cybersecurity. Like patient care, vigilant monitoring and quick response are vital. Organizations must be aware of potential threats and detect malicious endpoint activities. Securing network entry and exit points with robust endpoint protection ensures suspicious activity is quickly identified and mitigated.

This process involves:

- Threat Detection: Implement tools and protocols to detect threats at endpoints.
- Endpoint Protection: Secure entry and exit points to the network to prevent unauthorized access.

Threats Mitigated:

- Malware exploitation on endpoint devices
- Ransomware
- Lack of situational awareness of threat landscape
- Unplanned operational downtime

Actionable Steps:

Deploy advanced endpoint detection and response (EDR) solutions.

Regularly update and patch endpoint protection systems.

Conduct regular threat intelligence briefings to stay informed about the latest TTPs.

Train staff on recognizing and responding to endpoint security alerts.

Network Segmentation

Segmenting the network is like creating secure zones within a hospital where only authorized personnel can access specific areas. This approach protects mission-critical assets such as patient records and medical devices by preventing unauthorized users from moving freely within the network. By limiting access to sensitive information and systems, network segmentation reduces the risk of widespread damage during a cyberattack.

Actionable Steps:

Implement network segmentation for critical systems.

Conduct annual reviews of network segmentation.

Update segmentation policies based on new threats.

This process involves:

- Implementation of Segmentation: Use firewalls and VLANs to segment the network.
- Regular Reviews: Regularly review and update network segmentation policies.

Threats Mitigated:

- Asset compromise
- Lack of situational awareness of threat landscape
- Ransomware

Centralized Log Collection

Centralized collection of security logs is like having a comprehensive surveillance system for your network, allowing you to see and respond to potential threats quickly. By gathering all security logs in one place, you can easily monitor activities, detect unusual behavior, and take swift action to prevent breaches. This approach ensures you have a clear overview of your cybersecurity landscape.

Actionable Steps:

Deploy a centralized log management system.

Regularly review log data for suspicious activities.

Integrate log management with security information and event management (SIEM) systems.

This process involves:

- Log Management: Use centralized log management tools to collect and analyze logs.
- Incident Response: Integrate log management with incident response systems.

Threats Mitigated:

- Lack of situational awareness of threat landscape

Centralized Incident Planning and Preparedness

Centralized planning and preparedness for cybersecurity incidents ensure that all parts of an organization respond in a unified and efficient manner. Think of it like a fire drill—everyone knows their role and acts quickly to minimize damage. Regular practice and updates to the plan help keep everyone prepared for real emergencies, reducing chaos and downtime.

Actionable Steps:

Create a centralized incident response plan.

Schedule semi-annual incident response drills.

Update the plan based on drill outcomes and new threats.

This process involves:

- Incident Response Plan: Develop a centralized incident response plan.
- Regular Drills: Conduct regular drills to test the plan.

Threats Mitigated:

- Lack of situational awareness of threat landscape

Configuration Management

Maintaining secure configurations for all devices and systems is crucial to protecting against vulnerabilities. Think of it like ensuring all doors and windows in your house are securely locked to prevent intruders. Without proper configurations, your network is left open to cyber threats. This involves setting up and adhering to strict security guidelines, regularly updating systems, and conducting periodic audits to ensure compliance.

Actionable Steps:

Implement a configuration management system.

Develop secure configuration baselines.

Conduct quarterly configuration audits.

This process involves:

- Configuration Baselines: Establish and maintain secure configuration baselines.
- Regular Audits: Conduct regular audits to ensure compliance with configuration standards.

Threats Mitigated:

- Asset compromise
- Unplanned outages
- Unplanned operational downtime

Fortify Your Healthcare Cybersecurity

Protect, Respond, Recover with Xpio Health

Implementing essential and enhanced cybersecurity measures is crucial for healthcare organizations to protect their systems and patient data effectively. By following these actionable steps, organizations can build a robust cybersecurity posture that not only mitigates risks but also enhances their ability to respond to and recover from incidents.

At Xpio Health, we leverage continuous compliance through our advanced compliance platform and collaborate with top-tier vendors to deliver best-in-class solutions tailored to your needs. We are dedicated to partnering with healthcare organizations to achieve these goals and improve their overall cybersecurity resilience.

Contact us today to learn how we can help you strengthen your cybersecurity and optimize your EHR systems.

xpiohealth.com

info@xpiohealth.com
(888) 974-6408
3118 Judson Street
PO Box 498
Gig Harbor, Washington 98335 USA

Xpio HEALTH

xpiohealth.com

info@xpiohealth.com

(888) 974-6408

3118 Judson Street

PO Box 498

Gig Harbor,
Washington 98335

Improving the health of organizations and the people they serve